UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/563,504	06/23/2006	Udo Doebrich	2003P05083WOUS	8240

22116 7590 01/13/2009

SIEMENS CORPORATION
INTELLECTUAL PROPERTY DEPARTMENT
170 WOOD AVENUE SOUTH
ISELIN, NJ 08830

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
01/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/563,504	DOEBRICH ET AL.	
	Examiner	Art Unit	
	Christian LaForgia	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *24,28,30,33-35,37 and 40-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *24,28,30,33-35,37 and 40-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 29 October 2008 has been noted and made of record.

2. Claims 24, 28, 30, 33-35, 37, and 40-51 have been presented for examination.

3. Claims 25-27, 29, 31, 32, 36, 38, and 39 have been cancelled as per Applicant's amendment. The Examiner apologizes for the oversight in the previous office action of including claims 25, 27, and 29, and appreciates the Applicant's pointing out of this oversight.

Response to Arguments

4. Applicant's arguments filed 29 October 2008 have been fully considered but they are not persuasive.

5. The Applicant argues on page 10 that the Noguchi reference does not teach that the users transmit a random number. The Applicant contends that Noguchi discloses transmitting an encryption key in the abstract. While the Examiner agrees that this is disclosed in the abstract it appears that the Applicant disregards the cited portions of columns 9 and 12. Column 9, lines 41-50 states:

> Destination B encrypts the random number R for generating a symmetric key and an ID (hereinafter called "ID2") that specifies a symmetric key generation algorithm and sends them to source A. The transmission of ID2 between source A and destination B may be omitted like ID1, if ID2 is fixed such as when source A and destination B use the same communication software. At the same time, destination B generates a symmetric key Kc using the symmetric key generation algorithm.

The Applicant is reminded that prior art is relevant for all it contains, including non-preferred and alternative embodiments. See MPEP § 2123. Since Noguchi discusses generating a

symmetric key from a random value and transmitting that random value to the other user, the limitations of the claims have been met and the Applicant's arguments are not persuasive.

6. The Applicant argues that the invention of Noguchi could not be used on a public network or the Internet. It is noted that the features upon which applicant relies, namely that the communication network is a public network or the Internet, are not recited in the rejected independent claims. Although the claims are interpreted in light of the specification, limitations from the specification and dependent claims are not read into the independent claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The independent claims require a communication network; one of ordinary skill in the art would construe this as any type of communication network, including the "ad-hoc" communication network disclosed by Noguchi.

7. In response to applicant's argument that Noguchi has rare application, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

8. In response to applicant's argument that the combination of Gleeson and Noguchi would not support the present invention, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

9. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on

obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

10. See further rejections set forth below.

Claim Rejections - 35 USC § 103

11. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

12. Claims 24, 28, 30, 33-35, 37, 40, 42-45, 50, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 7,215,775 B2 to Noguchi et al., hereinafter Noguchi, in view of U.S. Patent No. 6,947,559 B2 to Gleeson, hereinafter Gleeson.

13. As per claims 24 and 40, Noguchi teaches a method and communication system for transmitting data, comprising:

providing each of a plurality of users of a communications network with a secret encryption program and a secret algorithm for generating an encryption key (column 9, lines 41-50, i.e. an ID that specifies key generation algorithm and different communication software that provides for different encryption programs);

by a first user of the communication network:

generating a first symmetrical encryption key based on the first random value using the secret algorithm (Figures 4, 10 [block 33], column 9, lines 41-50, column 12, lines 13-19);

a storage unit for storing the first symmetrical encryption key (Figure 10 [block 35], column 12, lines 22-25); and

transmitting the first random value to a second user of the communication network (Figures 4, 10 [block 31], column 9, lines 41-44, column 12, lines 17-22, i.e. sending a random number R and an ID that specifies an key generation algorithm to source A from destination B); by the second user:

receiving the first random value from the first user (Figures 4, 10 [block 31], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc); and

generating the first symmetrical encryption key based on the received random value using the secret algorithm (Figures 4, 10 [block 33], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc);

the first and second users then communicating encrypted data over the communications network using the secret encryption program and the first symmetrical encryption key (column 9, lines 57-59, i.e. cipher communications).

14. Noguchi does not teach wherein the random value is generated from a stochastic process, wherein the first rand value comprises a digital value derived from a sensor output of an operational measurement of an automation system.

15. Gleeson teaches measuring a physical property, such as absorbance, transmittance, reflectance, or current flow values which are than turned into a random number which is used to generate a key to encrypt data (column 2, lines 23-38, column 3, lines 4-13).

16. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the random value be generated from a stochastic process, since Gleeson states

at column 1, lines 7-20 that generating a random number in this manner are essential for strong data encryption, thereby preventing interlopers from gaining unauthorized access to the encrypted data.

17. Regarding claim 28, Gleeson teaches wherein the first stochastic process includes a time-variable parameter of an automation system (column 3, lines 44-62).

18. Regarding claims 30 and 42, Noguchi teaches wherein data transferred between the users is encrypted and unencrypted via the symmetrical encryption keys (Figure 4 [cipher communication using the symmetric keys]).

19. Noguchi and Gleeson do not disclose wherein the second user receives a second random value originating from a second stochastic process; generating a second symmetrical encryption key from a second stochastic process; transmitting the second random value to the first user; and the first user: receiving the second random value from the second user; and generating the second symmetrical encryption key based on the received random value.

20. It would have been obvious to one of ordinary skill in the art at the time the invention was made to duplicate the method of claims 24 and 40, respectively, for the second client, since it has been held that it only requires routine skill in the art to duplicate a method and that said duplication has no patentable significance unless new and unexpected results are produced. See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960).

21. With regards to claim 33, Noguchi teaches wherein one of the plurality of users is designated as a master user (column 13, line 28-62, i.e. PDA remotely controlling a laptop). Noguchi and Gleeson do not teach wherein the first and second symmetrical encryption keys are generated upon a request by a master user of the communication network.

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since the references do not disclose a third-party for initiating encrypted communications between the two parties.

23. With regards to claim 34, Gleeson teaches wherein the first and second symmetrical encryption keys are generated at predetermined times or after a lapse of a predetermined time interval (column 3, lines 44-62).

24. Regarding claim 35, Noguchi and Gleeson do not teach wherein the first random value are transmitted over the communication network at a time of low utilization of the communication network.

25. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit data over the network at a time of low utilization, since one of ordinary skill in the art would realize that retrieving information about the communication channel when utilization was low would provide for better results without interference from any cross communication occurring on the network.

26. Regarding claim 37, Noguchi teaches wherein the first random value is transmitted using an asymmetrical encryption method (column 9, lines 20-50, i.e. destination B encrypts the random number R using the public key Kp received from source A).

27. With regards to claim 43, Noguchi teaches wherein the communication network is the Internet (Figure 13 [elements 84, 92], column 13, lines 48-63).

28. Noguchi, Gleeson and Petersen do not teach that the first user is a master user for triggering the generating of the first and second symmetrical encryption keys by issuing a request via the Internet.

29. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since the references do not disclose a third-party for initiating encrypted communications between the two parties.

30. With regards to claim 44, Noguchi, Gleeson, and Petersen do not teach wherein the communication network is an Ethernet, and the first or second user is a master user configured to output a command onto the Ethernet for triggering the generation of the first and second symmetrical encryption keys.

31. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key

generation had to be triggered by one of the two users in order to establish encrypted communications since the references do not disclose a third-party for initiating encrypted communications between the two parties.

32. Regarding claim 45, Noguchi and Gleeson do not teach wherein the first random value is transmitted to the plurality of users and the first symmetrical encryption key is generated at each of the plurality of users using the secret algorithm.

33. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the first user transmit the random value to a plurality of users using the secret algorithm, especially so since Noguchi includes identifying which algorithm to use to generate the key, since one of ordinary skill in the art would recognize the need for providing secure communications in a group type setting.

34. Regarding claim 50, Gleeson teaches wherein the first random value comprises a combination of at least two digital values obtained from respective different sensors indicating respective different operational measurements of an automation system (column 3, line 47-62, coupling and mixing values).

35. With regards to claim 51, Gleeson teaches wherein the first random value comprises a concatenation of at least two digital values obtained from respective different sensors indicating respective different operational measurements of an automation system (column 3, line 47-62, coupling and mixing values).

36. Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Noguchi in view of Gleeson, and further in view of U.S. Patent Application Publication No. 2002/0154769 A1 to Petersen et al., hereinafter Petersen.

37. Regarding claim 41, Noguchi teaches wherein the communication network is a public network (Figure 13 [elements 84, 92], column 13, lines 48-63).

38. Noguchi and Gleeson do not teach removing at least one high order bit from the digital value to reduce a periodic component of the operation measurement.

39. Petersen teaches deleting the most significant bits from the digital value so that the value would fit in a designated register (paragraph 0039).

40. It would have been obvious to one of ordinary skill in the art at the time the invention was made to remove at least one high order bit from the digital value to reduce a periodic component of the operation measurement, since Petersen shows that removing high order bits is something well-known and commonly practiced. Something old does not become patentably distinct upon the discovery of a new property, such as reducing the periodic component of a measured value in the present case. The claiming of a new use, new function, or unknown property which is inherently present in the prior art does not necessarily make the claim patentable. See *In re Best*, 562 F.2d 1252, 1254, 195 USPQ 430, 433 (CCPA 1977); see also MPEP 2112(I).

41. Claim 46 is rejected under 35 U.S.C. 103(a) as being unpatentable over Noguchi in view of Gleeson in view of Petersen as applied above, and further in view of U.S. Patent No. 6,973,499 B1 to Peden et al., hereinafter Peden.

42. With regards to claim 46, Noguchi, Gleeson, and Petersen do not teach wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval.

43. Peden teaches wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval (column 6, lines 10-24, claim 18, i.e. a plurality of keys, wherein each key corresponds to one of a plurality of time intervals and each key being a symmetric key).

44. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the first symmetrical encryption key to be used to encrypt data transmitted during a first time interval and the second symmetrical encryption value to be used to encrypt data transmitted during a second time interval, since Peden states at column 2, lines 14-31 that designating keys for certain time periods prevents unauthorized users from accessing data in an environment that has a constantly changing base of users.

45. Claims 47-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noguchi in view of Gleeson, and further in view of U.S. Patent No. 6,973,499 B1 to Peden et al., hereinafter Peden.

46. As per claim 47, Noguchi teaches a method for transmitting data, comprising by a first user of a communication network:

storing a first random measured value (Figure 10 [block 35], column 12, lines 22-25);

generating a first symmetrical encryption key based on the first random measured value (Figures 4, 10 [block 33], column 9, lines 41-50, column 12, lines 13-19);

transmitting the first measured random value to a second user of the communication network (Figures 4, 10 [block 31], column 9, lines 41-44, column 12, lines 17-22, i.e. sending a random number R and an ID that specifies an key generation algorithm to source A from destination B);

by the second user:

receiving a first random measured value from the first user (Figures 4, 10 [block 31], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc);

generating the first symmetrical encryption key based on the received measured random value (Figures 4, 10 [block 33], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc).

47. Noguchi does not teach wherein the random value is generated from a stochastic process, wherein the first rand value comprises a digital value derived from a sensor output of an operational measurement of an automation system.

48. Gleeson teaches measuring a physical property, such as absorbance, transmittance, reflectance, or current flow values which are than turned into a random number which is used to generate a key to encrypt data (column 2, lines 23-38, column 3, lines 4-13).

49. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the random value be generated from a stochastic process, since Gleeson states at column 1, lines 7-20 that generating a random number in this manner are essential for strong data encryption, thereby preventing interlopers from gaining unauthorized access to the encrypted data.

50. Noguchi and Gleeson do not disclose wherein the second user receives a second random value originating from a second stochastic process; generating a second symmetrical encryption key from a second stochastic process; transmitting the second random value to the first user; and the first user: receiving the second random value from the second user; and generating the second symmetrical encryption key based on the received random value and wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval.

51. It would have been obvious to one of ordinary skill in the art at the time the invention was made to duplicate the method generating the first client's symmetric key for the second client, since it has been held that it only requires routine skill in the art to duplicate a method and that said duplication has no patentable significance unless new and unexpected results are produced. See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960).

52. Peden teaches wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval (column 6, lines 10-24, claim 18, i.e. a

plurality of keys, wherein each key corresponds to one of a plurality of time intervals and each key being a symmetric key).

53. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the first symmetrical encryption key to be used to encrypt data transmitted during a first time interval and the second symmetrical encryption value to be used to encrypt data transmitted during a second time interval, since Peden states at column 2, lines 14-31 that designating keys for certain time periods prevents unauthorized users from accessing data in an environment that has a constantly changing base of users.

54. Regarding claim 48, Gleeson teaches wherein the first random value is an input to a function and an output of the function is used to generate the first symmetrical encryption key (column 2, lines 23-38, column 3, lines 4-13).

55. Regarding claim 49, Gleeson teaches wherein the second random value is an input to a function and an output of the function is used to generate the second symmetrical encryption key (column 2, lines 23-38, column 3, lines 4-13).

Conclusion

56. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

57. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

58. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

59. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

60. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf